1 Question 1

1.1 Part a

$$P = (C \boxplus \bar{K_1}) \oplus K_0$$

where $\bar{K_1}$ is the complement of K_1.

1.2 Part b

Let our plaintext messages be P_a, P_b and their corresponding ciphertexts be C_a, C_b. We know that

$$C_a = (P_a \oplus K_0) \boxplus K_1$$
$$C_b = (P_b \oplus K_0) \boxplus K_1$$

We can define K_0 in terms of C_a, P_a, and K_1 by rearranging the variables.

$$(P_a \oplus K_0) \boxplus K_1 = C_a$$

$$P_a \oplus K_0 = C_a \boxplus \bar{K_1}$$
$$K_0 = (C_a \boxplus \bar{K_1}) \oplus P_a$$

Likewise,

$$K_0 = (C_b \boxplus \bar{K_1}) \oplus P_b$$

Which means

$$(C_a \boxplus \bar{K_1}) \oplus P_a = (C_b \boxplus \bar{K_1}) \oplus P_b$$
$$(C_a \boxplus \bar{K_1}) \oplus P_a \oplus P_b = C_b \boxplus \bar{K_1}$$
$$\big((C_a \boxplus \bar{K_1}) \oplus P_a \oplus P_b\big) \boxplus C_b = \bar{K_1}$$

We can then use $\bar{K_1}$ to find K_0 via

$$K_0 = (C_a \boxplus \bar{K_1}) \oplus P_a$$